

FIG. 1

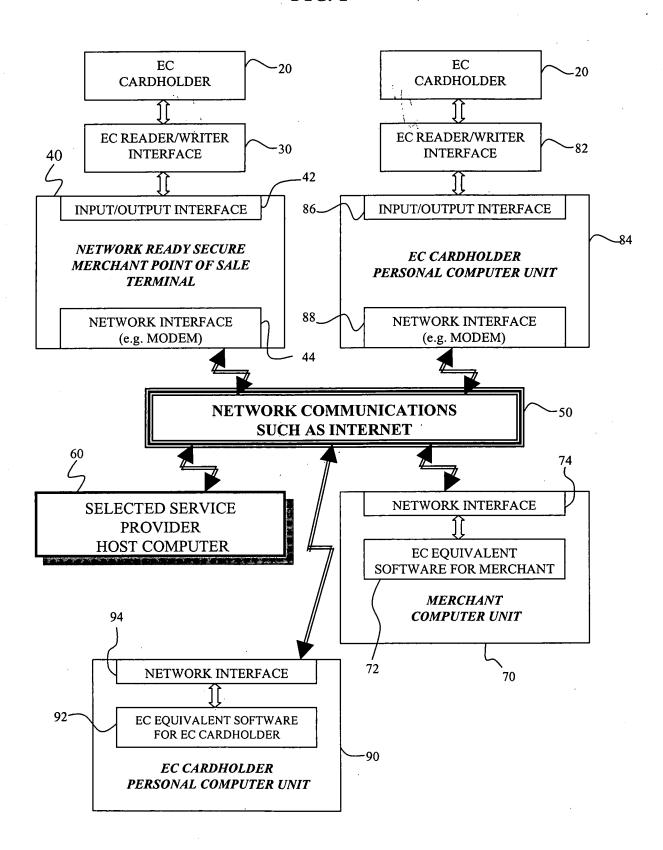
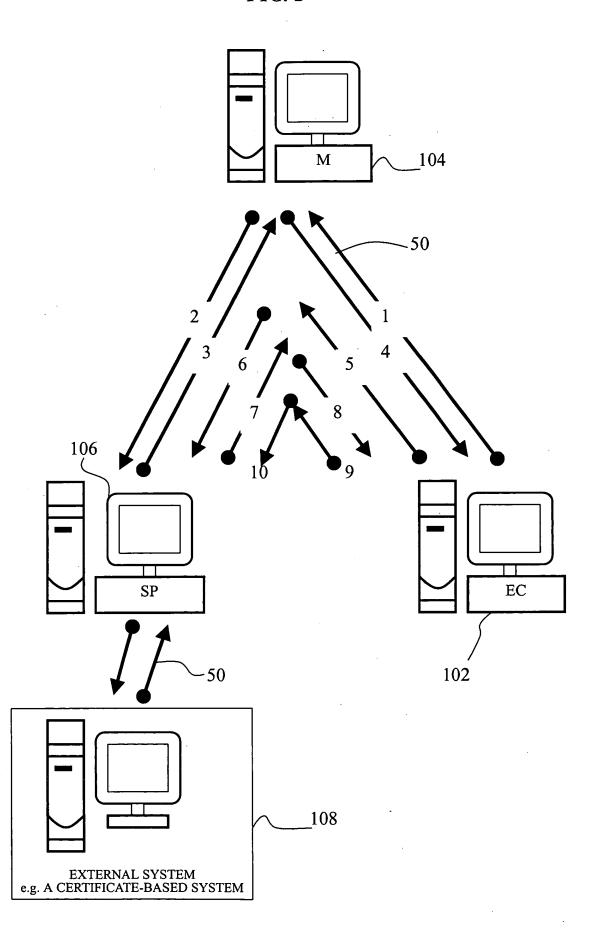


FIG. 2



COHMEZOH.IEGESO

ELECTRONIC CARD

			20 ELECTRONIC CARD									
		714	Miscellan- eous Data				·					
		712	PIN (optional)									
٠.	(SPDA)	710	CARD TYPE	CREDIT CARD	DEBIT CARD	ATM CARD	MEMBER CARD	LOYALTY CARD	etc.			
FIG. 4	SERVICE PROVIDERS' DATA AREA (SPDA)	708	ACCOUNT INFORMATION (Number, expiration date, etc.)									
	SERVICE	902	KEY									
		704	KEY									
6 7		702	NAME									

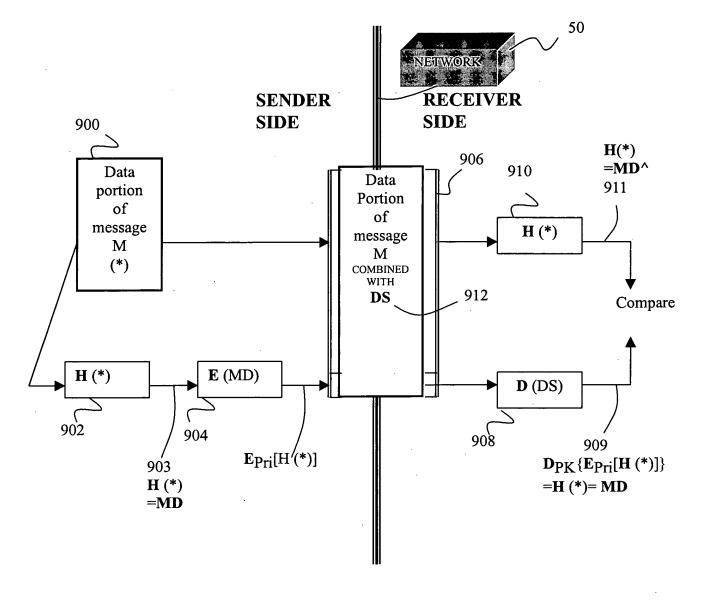


FIG. 6A **START** 110 EC CARDHOLDER ENTERS CARD ACCESS CONDITIONS 112 114 116 STORED CARD MATCHED? REJECTED ACCESS CONDITIONS NO YES 118 UNLOCK EC CARD FOR USE -120 EC SELECTS A SERVICE PROVIDER FROM ITS SERVICE PROVIDER DATA AREA (SPDA) SP-PK READ EC'S PUBLIC KEY PKEC 124 RANDOM NUMBER GENERATOR EC'S SENSITIVE GENERATES EC'S RN_{EC} 126 TRANSACTION DATA: STD_{EC} 128 $\label{eq:RN} \mathsf{EC}$ PK_{EC} STD_{EC} EC'S ENCIPHIR: USE SELECTED SERVICE PROVIDER PUBLIC KEY ENCRYPTS $\mathbf{E}_{\text{SP-PK}}(\text{RN}_{\text{EC}}*\text{PK}_{\text{EC}}*\text{STD}_{\text{EC}})$ 122 EC PLAIN TEXT: EC COMBINES PLAIN TEXT AND CRYPTOGRAM: $PLAIN\ TEXT_{EC}*E_{SP\text{-}PK}(RN_{EC}*PK_{EC}*STD_{EC})$ PLAIN TEXT_{EC} - 130 132 EC HASHES AND PRODUCES A MESSAGE DIGEST MD_{EC}: $H[PLAIN TEXT_{EC}*E_{SP-PK}(RN_{EC}*PK_{EC}*STD_{EC})]=MD_{EC}$ - 134 TO STEP 140 FIG. 6B

TO STEP136 FIG. 6B

FIG. 6B

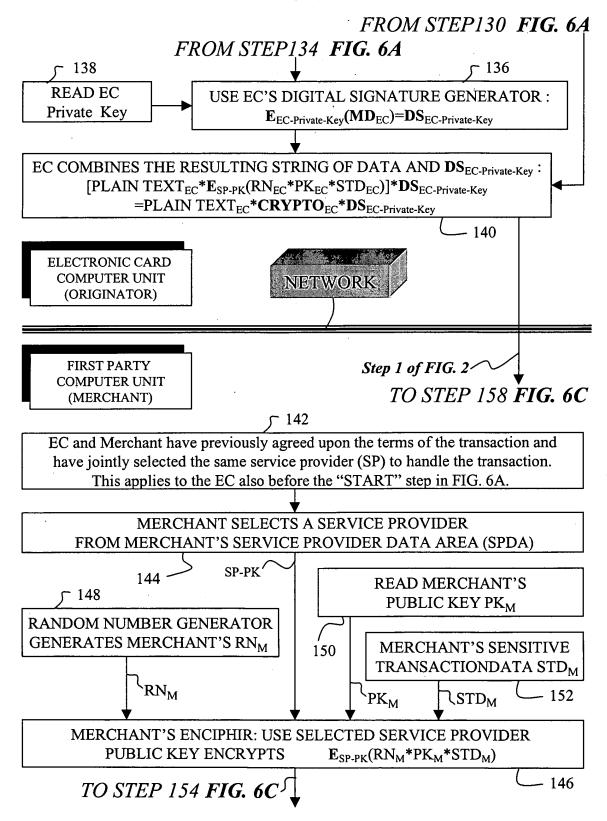
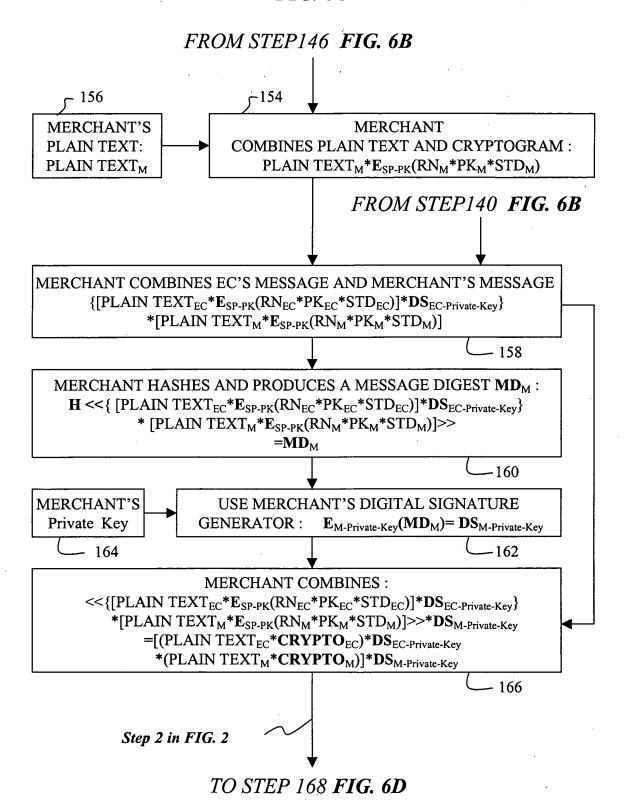


FIG. 6C



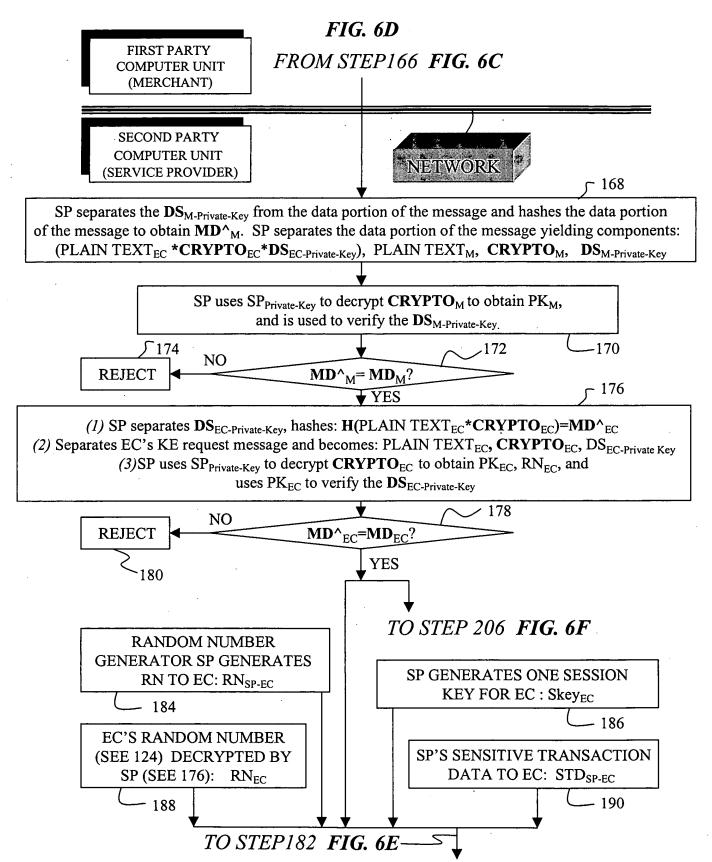


FIG. 6E

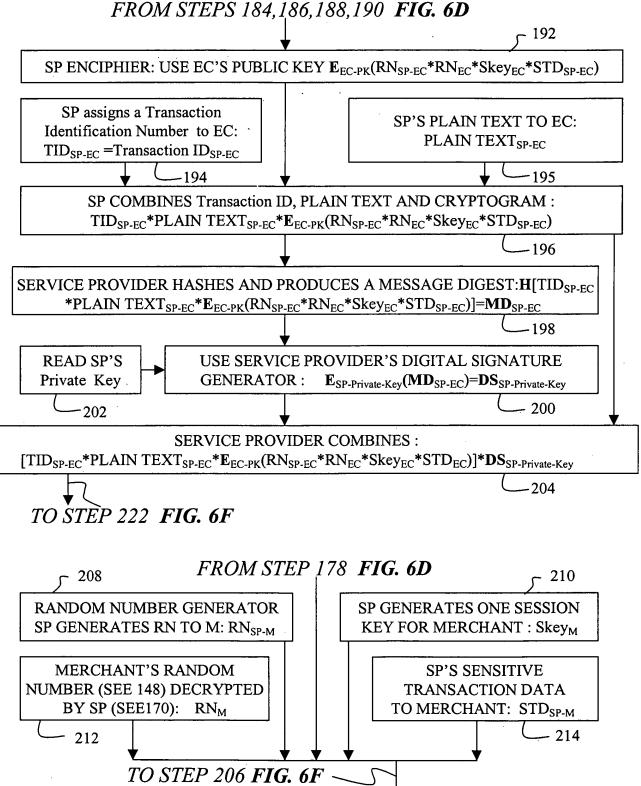
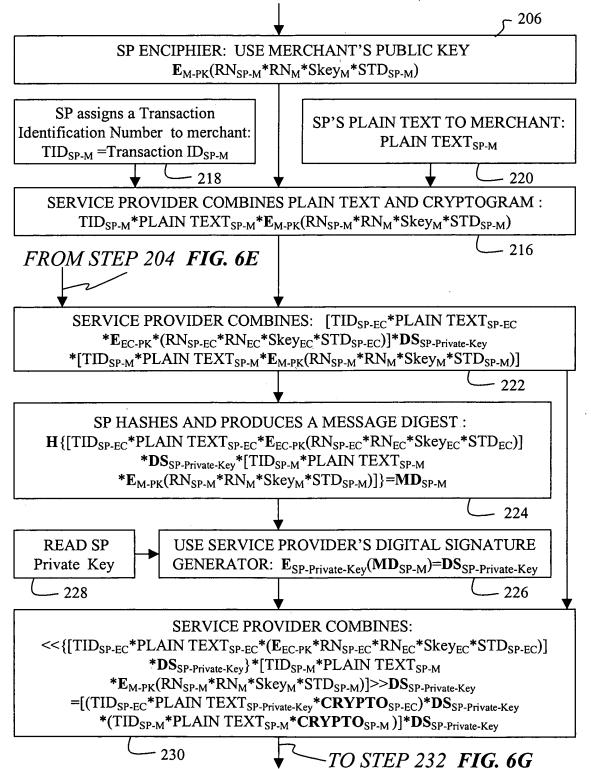


FIG. 6F FROM STEPS 208,210, 212,214 FIG 6E



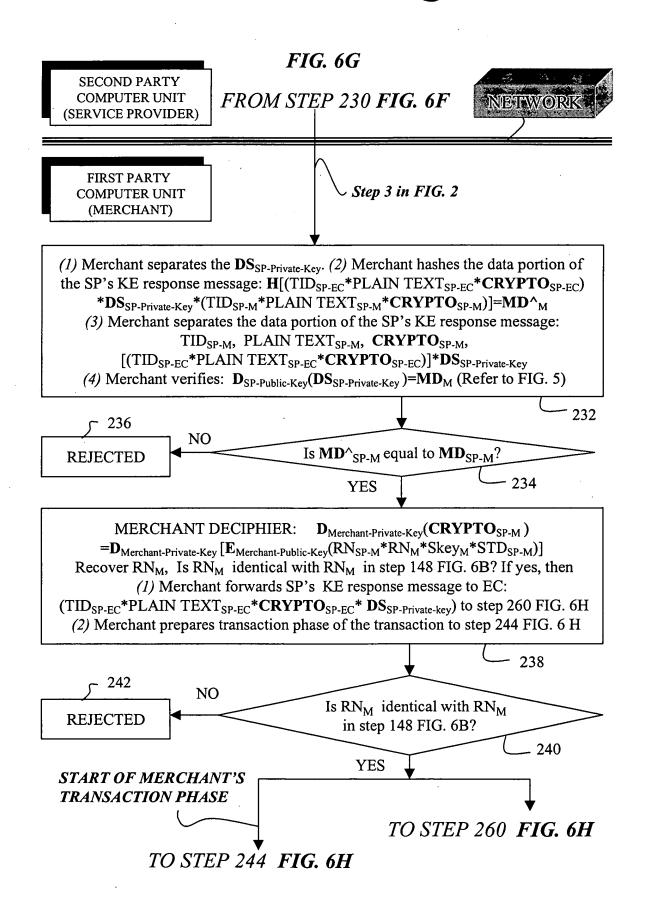


FIG. 6H

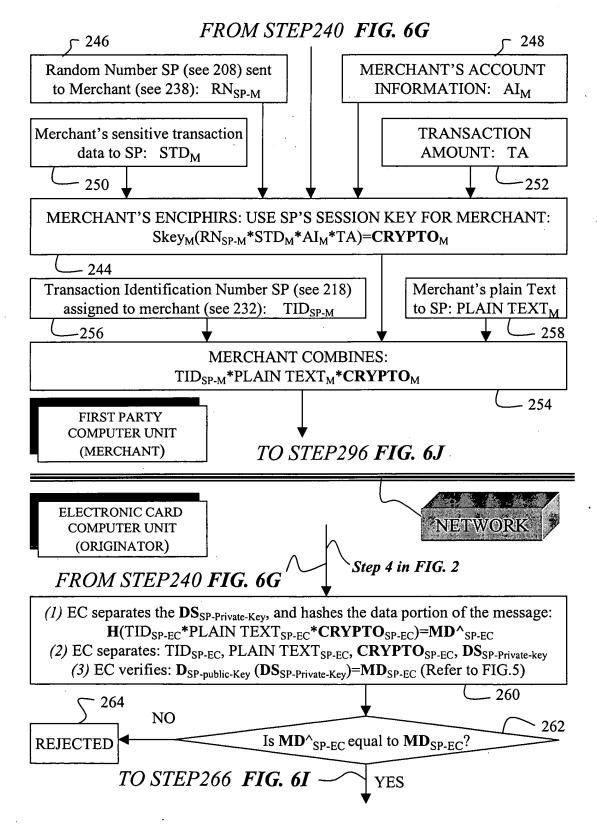
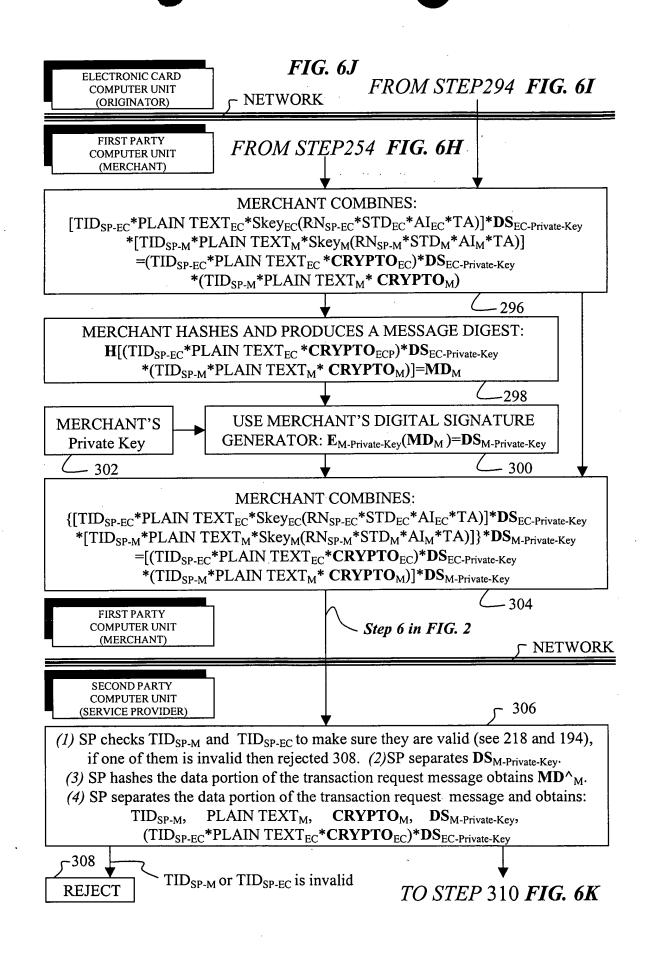


FIG. 61 FROM STEP262 FIG. 6H 266 EC'S DECIPHIER: **D**_{EC-Private-Key}(**CRYPTO**_{SP-EC})=**D**_{EC-Private-Key} [E_{EC-Public-Kev}(RN_{SP-EC}*RN_{EC}*Skey_{EC}*STD_{SP-EC})]; And recovers RN_{EC} 268 NO Is RN_{EC}=RN_{EC} REJECTED in step 124 FIG. 6A? YES 274 START OF EC'S TRANSACTION PHASE RANDOM NUMBER SP (see 184) EC'S ACCOUNT INFORMATION: AI_{EC} SENT TO EC (see 266): RN_{SP-EC} SENSITIVE TRANSACTION **TRANSACTION** 276 DATA EC TO SP: STD_{EC} AMOUNT: TA 278 280 EC'S ENCIPHIR: USE SP'S SESSION KEY FOR EC: $Skey_{EC}(RN_{SP-EC}*STD_{EC}*AI_{EC}*TA)=CRYPTO_{EC}$ 272 Transaction Identification Number SP (see 194) EC's PLAIN TEXT: assigned to EC (see 260): TID_{SP-EC} PLAIN TEXT_{EC} 284 286 TID_{EC}*PLAIN TEXT_{EC}*CRYPTO_{EC} EC COMBINES: - 282 EC HASHES AND PRODUCES A MESSAGE DIGEST: $H[TID_{SP-EC}*PLAIN TEXT_{EC}*CRYPTO_{EC}]=MD_{EC}$ - 288 READ EC'S USE EC'S DIGITAL SIGNATURE GENERATOR: $\mathbf{E}_{\text{EC-Private-Key}}(\mathbf{MD}_{\text{EC}}) = \mathbf{DS}_{\text{EC-Private-Key}}$ Private Key - 292 290 $[TID_{SP-EC}*PLAIN TEXT_{EC}$ EC COMBINES: $*Skey_{EC}(RN_{SP-EC}*STD_{EC}*AI_{EC}*TA)]*\mathbf{DS}_{EC-Private-Key}$ - 294 Step 5 in FIG. 2

TO STEP296 FIG. 6J



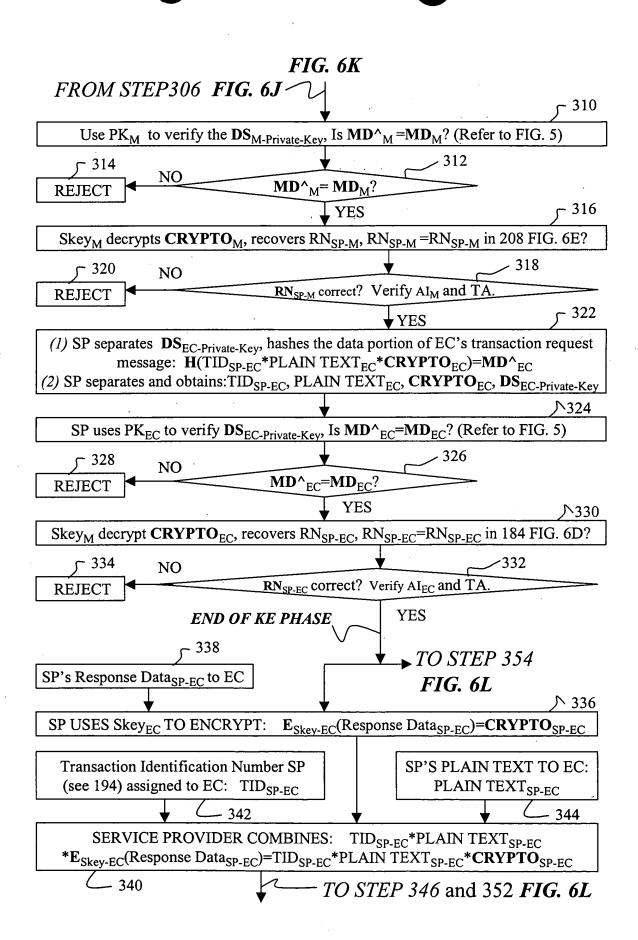


FIG. 6L

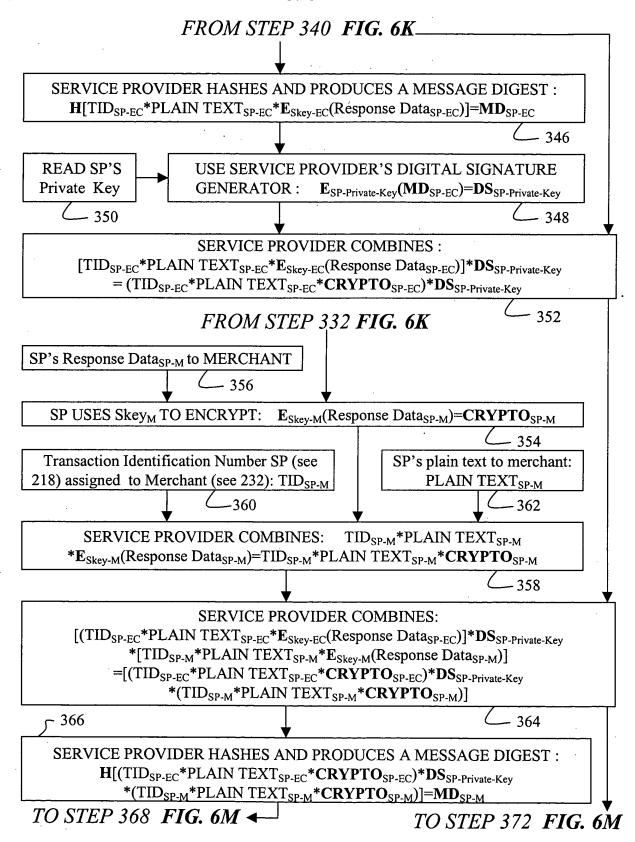


FIG. 6M

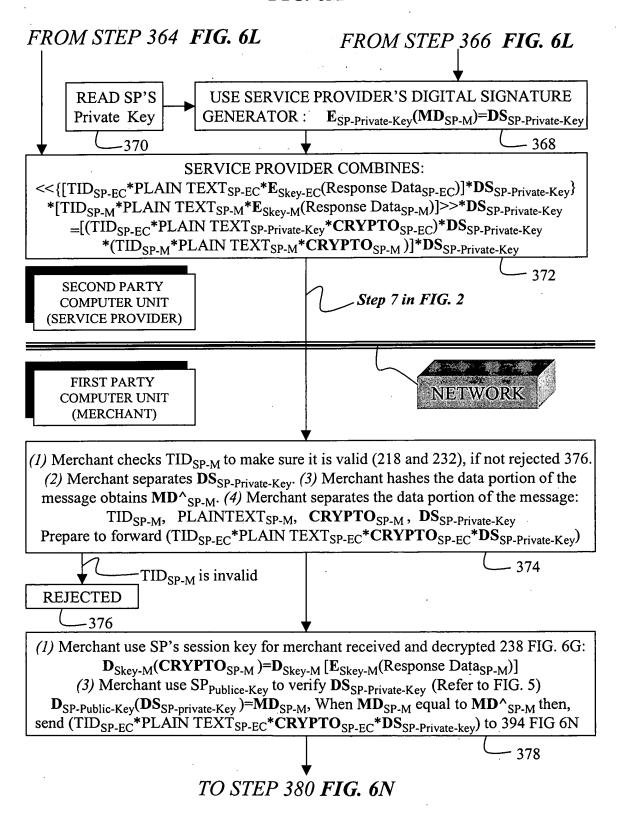
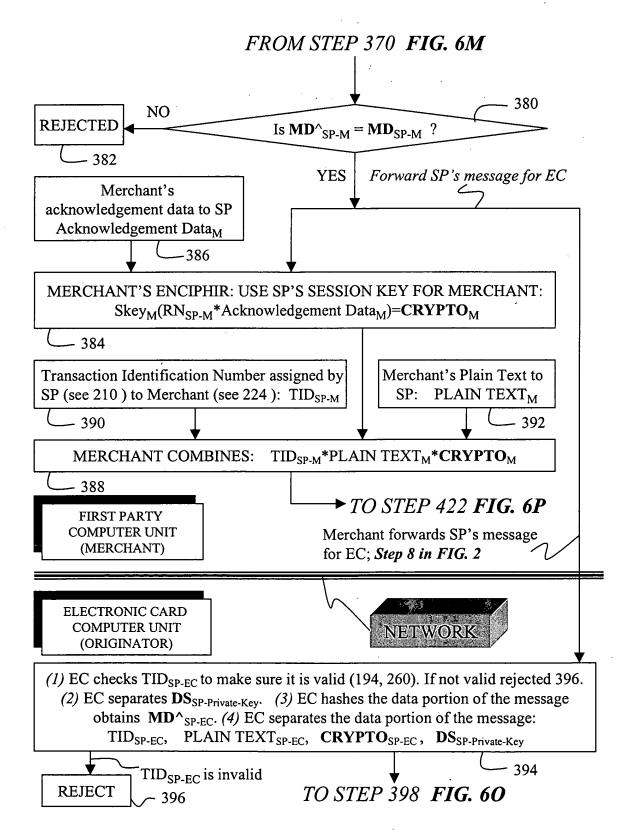
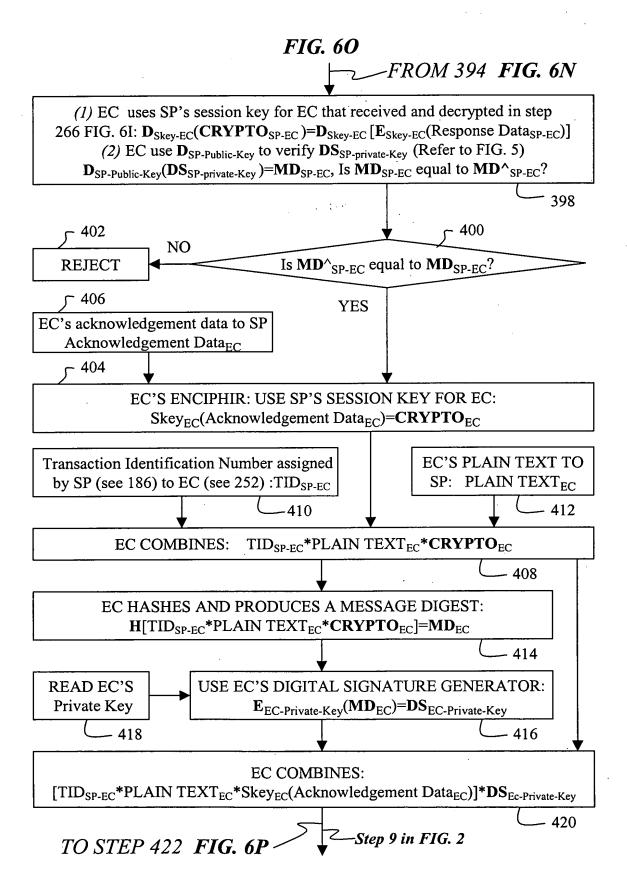


FIG. 6N





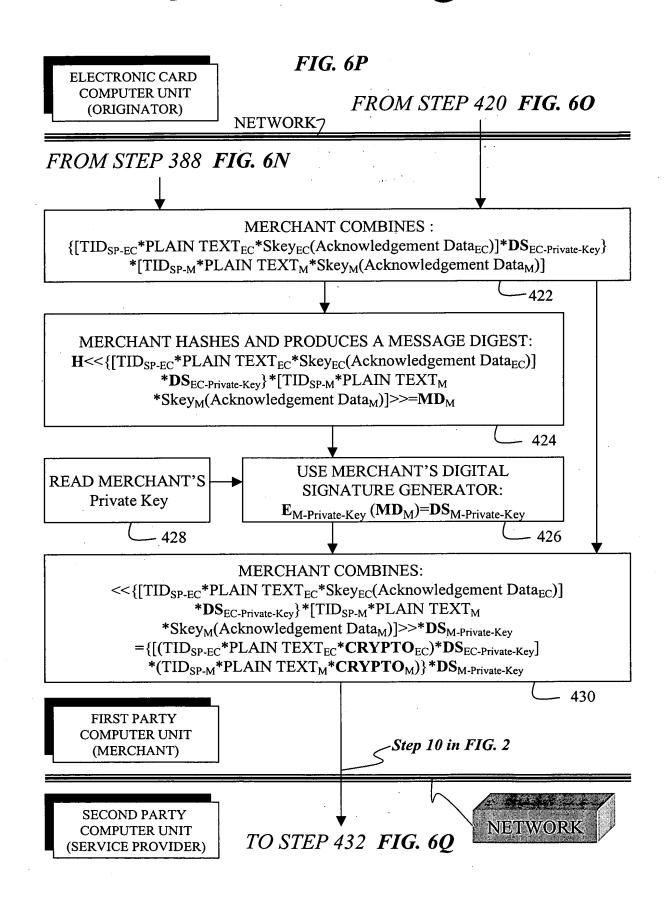


FIG. 6Q

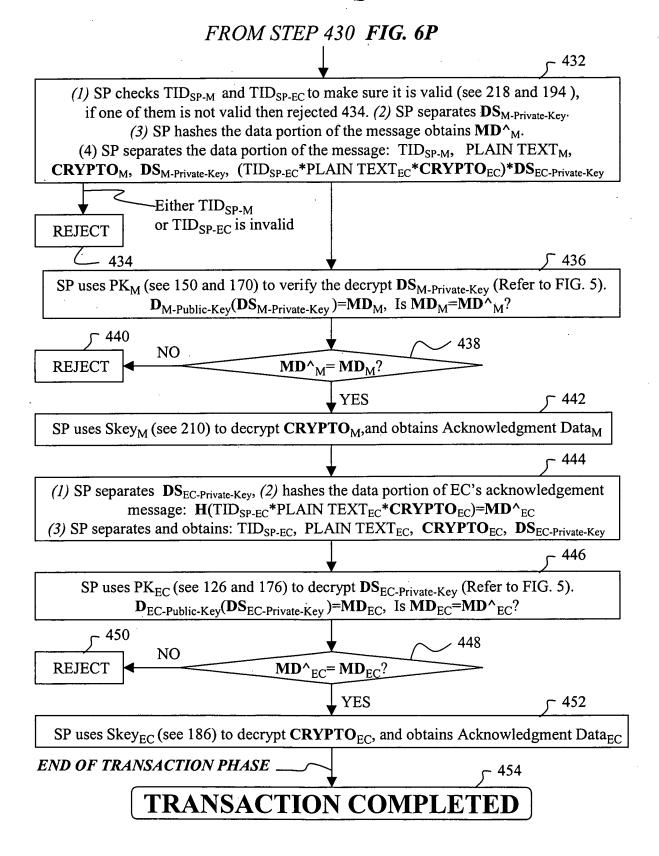


FIG. 7

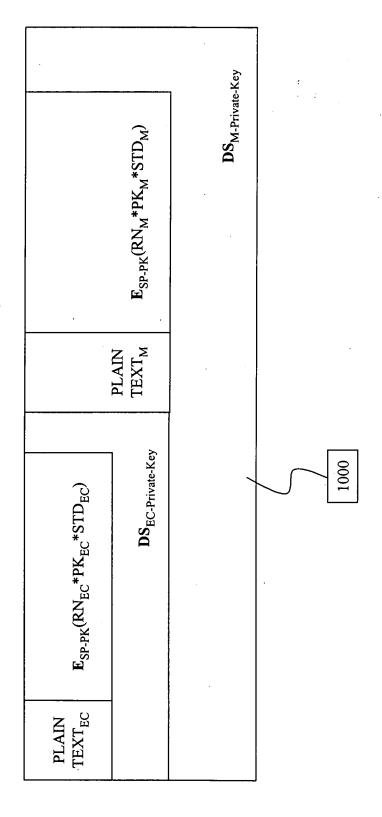


FIG.8

	·		\neg
E _{M-PK} (RN _{SP-M} *RN _M *Skey _M	$^*\mathrm{STD}_{\mathrm{SP-M}}$	DS _{SP-Private-Key}	
Transaction Identification	Number _{SP-M} TID _{SP-M}		
	PLAIN TEXT _{SP-M}		
E _{EC-PK} (RN _{SP-EC} *RN _{EC} *Skey _{EC} *STD _{SP-EC})	DS _{SP-Private-Key}		1020
Transaction Identification Number _{SP-EC} TID _{SP-EC}			
PLAIN TEXT _{SP-EC}			

FIG. 9

			· ¬
ESkey-M(RNSP-M	$^*_{\mathrm{AI}_{\mathrm{M}}}$ $^*_{\mathrm{STD}_{\mathrm{M}}}$ $^*_{\mathrm{TA}}$	DS _M -Private-Key	
	Identification Number _{SP-M} TID _{SP-M}		
	${ m PLAIN} \ { m TEXT}_{ m M}$		
E _{Skey-EC} (RN _{SP-EC} *Al _{EC} *STD _{EC} *TA)	DS _{EC-Private-Key}		1040
Transaction Identification Number _{SP-EC} TID _{SP-EC}			
PLAIN TEXT _{EC}			

FIG.10

	$\mathbf{E}_{\mathrm{Skey-M}}(\mathrm{Response})$ Data _{SP-M})	DS _{SP-Private-Key}	
Transaction Identification	Number _{SP-M} TID _{SP-M}	,	
	PLAIN TEXT _{SP-M}		
E _{Skey-EC} (Response Data _{SP-EC})	DS _{SP-Private-Key}		1060
Transaction Identification Number _{SP-EC} TID _{SP-EC}			
PLAIN TEXT _{SP-EC}			

FIG.11

			, , , , , , , , , , , , , , , , , , , ,	
E _{Skey-M} (Acknowledgement	$Data_M$)		DS M-Private-Key	
Transaction Identification	·		·	
$\mathbf{E}_{ ext{Skey-EC}}$ (Acknowledgement Data $_{ ext{EC}}$)	DS _{EC-Private-Key}			1080
Transaction Identification Number _{SP-EC} TID _{SP-EC}		·		
PLAIN TEXT _{EC}				

FIG. 12

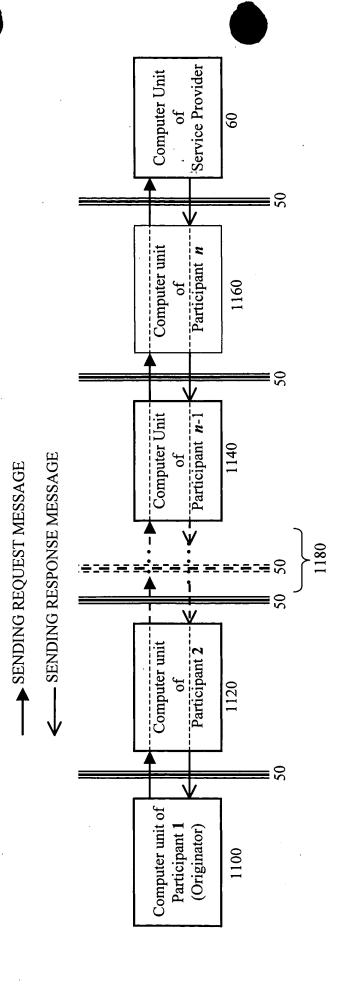


FIG. 13

